Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) In a cryptographic system wherein a certifying authority issues digital certificates identifying users of said system, said digital certificates being digitally signed with a private key of said certifying authority to form a digital signature and requiring a public key of said certifying authority in order to verify said digital signature, and wherein a user transaction in said cryptographic system requires verification by a recipient of said user transaction, said verification based on information in said digital certificates and requiring said public key, a method of controlling use of said public key comprising:

by said recipient, digitally signing at least one message containing rules of said system, by which said recipient agrees to said rules, said rules including a rule regarding maintaining secrecy of said public key; and

in response to said digital signing, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization of said public key.

2. – 17. (Canceled)

18. (Previously Presented) The method of claim 1, wherein said recipient has a secure device containing said public key, wherein said public key cannot be obtained from said secure device.

19. (Previously Presented) The method of claim 1, wherein each user of the system has a private key, and wherein said rules include:

a rule requiring payment to a third party upon each use of said public key;

a rule requiring payment to a third party upon each use of a user's private key;

a rule requiring payment to a third party upon each certification of a certificate's status; or

a rule requiring payment to a third party upon each confirm-to transaction by a user.

20. (Previously Presented) The method of claim 1, wherein said rules include a rule to pay for use by said recipient of intellectual property provided through the system.

21. (Previously Presented) The method of claim 1, wherein said user transaction is invalid until said digital signing is performed.

22. - 71. (Canceled)

72. (Previously Presented) The method of claim 1, further comprising:

in response to said signing by said recipient, said certifying authority accepting a transaction from said recipient, said transaction based on said user transaction.

73. (Previously Presented) A method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key utilizable by a plurality of users of the cryptographic system, said method comprising:

in response to a recipient digitally signing a message containing rules of said cryptographic system, by which said recipient agrees to said rules, permitting said recipient to utilize said public key, said rules including a rule regarding maintaining secrecy of said public key; and

prior to said recipient digitally signing said message, denying use of said public key.

74. (Previously Presented) The method of claim 73, wherein said recipient has a secure device containing said public key, wherein said public key cannot be obtained from said secure device.

75. (Previously Presented) The method of claim 73, wherein each user of the system has a private key, and wherein said rules include:

a rule requiring payment to a third party upon each use of said public key;

a rule requiring payment to a third party upon each use of a user's private key;

a rule requiring payment to a third party upon each certification of a certificate's status; or

a rule requiring payment to a third party upon each confirm-to transaction by a user.

76. (Previously Presented) The method of claim 73, wherein said rules include a rule to pay for use by said recipient of intellectual property provided through the system.

77. (Previously Presented) The method of claim 73, wherein a user transaction of said recipient in the system is invalid until said digital signing is performed.

78. (Previously Presented) The method of claim 73, further comprising:

in response to said signing by said recipient, a certifying authority accepting a transaction from said recipient, said transaction based on a user transaction of said recipient in the system.

79. (Currently Amended) A method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key, said method comprising:

providing a recipient with a message containing rules of said system and with a secure hardware device containing an inactive form of said public key, wherein said public key cannot be obtained from said secure hardware device; and

in response to said recipient digitally signing said message, activating said public key in said secure hardware device.

80. (Previously Presented) The method of claim 79, wherein said public key is a public key of a certifying authority, said providing is performed by a certifying authority, said digitally signing comprises hashing said message to obtain a hashed document, digitally signing said hashed document to form a digital agreement, and returning said digital agreement to said certifying authority, and said activating is performed by said certifying authority.

81. (Previously Presented) The method of claim 79, wherein each user of the system has a private key, and wherein said rules include:

a rule requiring payment to a third party upon each use of said public key;

a rule requiring payment to a third party upon each use of a user's private key;

a rule requiring payment to a third party upon each certification of a certificate's status; or

a rule requiring payment to a third party upon each confirm-to transaction by a user.

82. (Previously Presented) The method of claim 79, wherein said rules include a rule to pay for use by said recipient of intellectual property provided through the system.

83. (Previously Presented) The method of claim 79, wherein a user transaction by said recipient in the system is invalid until said digital signing is performed.

84. (Previously Presented) The method of claim 79, further comprising:

in response to said signing by said recipient, a certifying authority accepting a transaction from said recipient, said transaction based on a user transaction of said recipient in the system.

85. – 108. (Cancelled)

109. (Previously Presented) The method of claim 79, where, in the cryptographic system, a certifying authority issues digital certificates identifying participants of the cryptographic system, the digital certificates being digitally signed with a private key of the certifying authority to form a digital signature and requiring a public key of the certifying authority in order to verify the digital signature, and a participant transaction requires verification by a recipient of the participant transaction, the verification based on information in a digital certificate and requiring the public key.

110. (Currently Amended) The method of claim 79, wherein the public key in the secure hardware device becomes inactive after a certain time period, the method further comprising:

after the public key becomes inactive,

in response to a demonstration by the recipient of agreement or consistency with one or more of the rules, activating the inactive public key in the secure hardware device.

111. (Currently Amended) The method of claim 110, wherein said demonstration includes information from the secure hardware device identifying operational capabilities of the secure hardware device and further including information uniquely binding said recipient to said demonstration by the recipient of agreement or consistency with one or more of the rules.

112. (Previously Presented) The method of claim 79, wherein the public key is certified by an authority.

113. (Previously Presented) The method of claim 79, further comprising:

a certifying authority accepting a transaction from the recipient, the transaction based on a transaction of the recipient in the cryptographic system, after demonstration by the recipient of agreement or consistency with one or more of the rules.

114. (Previously Presented) The method of claim 79, wherein the rules comprise a rule regarding maintaining secrecy of the public key.

115. (Currently Amended) The method of claim 79, wherein said activating comprises:

activating said public key in said secure hardware device in response to a predetermined transaction with said secure hardware device, said predetermined transaction including information from the secure hardware device identifying operational capabilities of the secure hardware device and uniquely identifying said secure hardware device and further including information uniquely binding said recipient to said predetermined transaction.

116. (Previously Presented) The method of claim 1, wherein the public key becomes inactive after a certain time period, the system further comprising:

after the public key becomes inactive,

in response to a demonstration by the recipient of agreement or consistency with one or more of the rules, activating the inactive public key.

117. (Currently Amended) The method of claim 116, wherein said demonstration includes information identifying operational capabilities of a secure hardware device and further including information uniquely binding said recipient to said demonstration by the recipient of agreement or consistency with one or more of the rules.

118. (Previously Presented) The method of claim 1, wherein the public key is certified by an authority.

119. (Previously Presented) The method of claim 1, wherein said permitting comprises making the public key available by providing access to an inaccessible public key.

120. (Previously Presented) The method of claim 1, further comprising:

a certifying authority accepting a transaction from the recipient, the transaction based on a transaction of the recipient in the cryptographic system, after demonstration by the recipient of agreement or consistency with one or more of the rules.

121. (Previously Presented) The method of claim 1, wherein said permitting comprises:

in response to a predetermined transaction with a secure device, activating said public key in said secure device, said predetermined transaction including information from the secure device identifying operational capabilities of the secure device and uniquely identifying said secure device and further including information uniquely binding said recipient to said predetermined transaction, wherein said public key cannot be obtained from said secure device.

122. (Previously Presented) The method of claim 73, wherein a secure device contains an inactive form of said public key and said permitting comprises activating said inactive public key in said secure device.

123. (Previously Presented) The method of claim 73, wherein said permitting comprises transferring said public key to said secure device.

124. (Previously Presented) The method of claim 73, wherein said public key is provided in a secure device.

125. (Previously Presented) The method of claim 124, wherein said public key in said secure device becomes inactive after a certain time period, said method further comprising:

after said public key becomes inactive,

in response to a demonstration by the recipient of agreement or consistency with one or more of the rules, activating said inactive public key in said secure device.

126. (Previously Presented) The method of claim 125, wherein said demonstration includes information identifying operational capabilities of the secure device and further including information uniquely binding said recipient to said demonstration by the recipient of agreement or consistency with one or more of the rules.

127. (Previously Presented) The method of claim 73, wherein said permitting comprises transferring the public key to a secure device, wherein the public key cannot be obtained from the secure device.

128. (Previously Presented) The method of claim 73, where, in the cryptographic system, a certifying authority issues digital certificates identifying participants of the cryptographic system, the digital certificates being digitally signed with a private key of the certifying authority to form a digital signature and requiring a public key of the certifying authority in order to verify the digital signature, and a participant transaction requires verification by a recipient of the participant transaction, the verification based on information in a digital certificate and requiring the public key.

129. (Previously Presented) The method of claim 73, further comprising:

a certifying authority accepting a transaction from the recipient, the transaction based on a transaction of the recipient in the cryptographic system, after demonstration by the recipient of agreement or consistency with one or more of the rules.

130. (Previously Presented) The method of claim 73, wherein said permitting comprises making the public key available by activating an inactive public key.

131. (Previously Presented) The method of claim 73, wherein said permitting comprises:

in response to a predetermined transaction with a secure device, activating said public key in said secure device, said predetermined transaction including information from the secure device identifying operational capabilities of the secure device and uniquely identifying said secure device and further including information uniquely binding said recipient to said predetermined transaction, wherein said public key cannot be obtained from said secure device.